PCT/DE 2004/000224

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 12 774.7

Anmeldetag: 21. März 2003

Anmelder/Inhaber: Deutsche Telekom AG, Bonn/DE

Bezeichnung: Verfahren und Kommunikationssystem zur Freigabe einer Datenverarbeitungseinheit

IPC: H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 28. August 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Slremme

A 9161
03/00
EDV-L

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Verfahren und Kommunikationssystem zur Freigabe einer Datenverarbeitungseinheit

Die Erfindung betrifft ein Verfahren und ein Kommunikationssystem zur Freigabe einer Datenverarbeitungseinheit zur Verarbeitung von Projektdaten eines ausgewählten Projekts.

Ein Anwendungsgebiet für die vorliegende Erfindung ist die kostenpflichtige Nutzung einer Software für die Verarbeitung eines Projekts.

Ein technisches Problem der Erfindung ist darin zu sehen, ein Verfahren sowie ein Kommunikationssystem zur Verfügung zu stellen, welches eine projektabhängige Freigabe oder Nutzung einer Datenverarbeitungseinheit ermöglicht.

Ein Grundgedanke der Erfindung ist darin zu sehen, dass ein Kunde Projektdaten eines bestimmten Projekts mit Hilfe einer Soft- und/oder Hardwarekomponente, nachfolgend auch Datenverarbeitungseinheit genannt, be- oder verarbeiten lassen möchte. Allerdings muss sich der Kunde erst ein Nutzungsrecht zur Nutzung der Datenverarbeitungseinheit zur Verarbeitung des einen bestimmten Projekts besorgen. Demzufolge wird ein bestimmtes Freigabesignal erzeugt, welches die Datenverarbeitungseinheit veranlasst, nur die zu dem Projekt gehörenden Projektdaten zu verarbeiten. Die Datenverarbeitungseinheit verarbeitet keine anderen Daten, solange für diese Daten kein Nutzungsrecht für die Nutzung der Datenverarbeitungseinheit vorliegt.

Das oben genannte technische Problem wird zum einen durch ein Verfahren gemäß Anspruch 1 gelöst.

Danach fordert ein Kunde das Nutzungsrecht für die Nutzung einer Datenverarbeitungseinheit an, um die zu einem vorbestimmten Projekt gehörenden Projektdaten zu verarbeiten. Anschließend wird eine erste Signatur erzeugt, indem die vorbestimmten, zu dem Projekt gehörenden Projektdaten insbesondere von einer Signatureinrichtung signiert werden. Die erste Signatur wird auf Korrektheit hin verifiziert. Die Datenverarbeitungseinheit wird nur dann freigegeben, die zum ausgewählten Projekt gehörenden Projektdaten zu verarbeiten, wenn die erste Signatur als korrekt verifiziert worden ist.

Zweckmäßigerweise ist die dem Kunden zugeordnete Datenverarbeitungseinheit, die Bestandteil eines Computers sein kann, über ein Kommunikationsnetz mit der Signatureinrichtung verbunden. In diesem Fall können die vorbestimmten Projektdaten beispielsweise per E-Mail über das Kommunikationsnetz zu einer Nutzungserlaubnis-Erzeugungseinrichtung übertragen werden, in der die erste Signatur erzeugt wird. Die Nutzungserlaubnis-Erzeugungseinrichtung kann ein Computer des Herstellers oder Anbieters der Datenverarbeitungseinheit sein.

Um sicherstellen zu können, dass die vorbestimmten Projektdaten bei der Übertragung zur Nutzungserlaubnis-Erzeugungseinrichtung und auch vor der Nutzungserlaubnis-Erzeugungseinrichtung selbst geheim bleiben, werden die vorbestimmten Projektdaten unter Anwendung einer Hashfunktion kryptografisch gesichert. Die vorbestimmten, kryptografisch gesicherten Projektdaten werden dann über das Kommunikationsnetz zur Nutzungserlaubnis-Erzeugungseinrichtung übertragen, wobei die erste Signatur dadurch erzeugt wird, dass die vorbestimmten, kryptografisch

gesicherten Projektdaten von der Signatureinrichtung signiert werden.

Die Hashfunktion komprimiert die vorbestimmten Projektdaten zu einem Hashwert. Ein Hashwert zeichnet sich dadurch aus, dass aus diesem Hashwert nicht auf die ursprünglichen Projektdaten geschlossen werden kann. Ferner haben Hashwerte die Eigenschaft, dass keine zwei verschiedene Projektdaten gefunden werden können, die den gleichen Hashwert ergeben.

Damit sich der Anbieter der Datenverarbeitungseinheit vergewissern kann, dass die vorbestimmten Projektdaten, die zur Freigabe der Datenverarbeitungseinheit signiert werden müssen, von einem bestimmten Kunden kommen, wird kundenseitig eine zweite Signatur erzeugt, indem die vorbestimmten Projektdaten signiert werden. Die vorbestimmten Projektdaten und die zweite Signatur werden dann zur Nutzungserlaubnis-Erzeugungseinrichtung übertragen. In der Nutzungserlaubnis-Erzeugungseinrichtung wird die zweite Signatur auf Korrektheit hin verifiziert. Die Signatureinrichtung erzeugt eine erste Signatur aus den vorbestimmten Projektdaten nur dann, wenn die zweite Signatur korrekt ist.

In ähnlicher Weise kann kundenseitig eine zweite Signatur erzeugt werden, indem die vorbestimmten, zuvor kryptografisch gesicherten Projektdaten signiert werden. Wiederum werden die vorbestimmten, kryptografisch gesicherten Projektdaten und die zweite Signatur zur Nutzungserlaubnis-Erzeugungseinrichtung übertragen. In der Nutzungserlaubnis-Erzeugungseinrichtung wird die zweite Signatur auf Korrektheit hin verifiziert. Die erste Signatur wird aus den vorbestimmten, kryptografisch gesicherten Projektdaten nur dann erzeugt, wenn die zweite Signatur korrekt ist.

Gemäß einer Weiterbildung der Erfindung kann die Projekt-abhängige Nutzung der Datenverarbeitungseinheit kostenpflichtig sein. Daher wird in Abhängigkeit von den vorbestimmten Projektdaten eines ausgewählten Projekts ein Rechnungsdatensatz zur Nutzung der Datenverarbeitungseinheit erzeugt. Dieser Rechnungsdatensatz entspricht einer Rechnung, die vom Kunden beglichen werden muß. Die Höhe der Rechnung, die dem Rechnungsdatensatz entspricht, kann davon abhängen, wieviele und welche Projektdaten von dem Kunden oder dem Anbieter der Datenverarbeitungseinheit als vorbestimmte Projektdaten definiert werden.

Um eine kostenpflichtige Nutzung der Datenverarbeitungseinheit zu ermöglichen, kann alternativ der Kunde zunächst mehrere Werteinheiten im voraus kaufen, die bei Anforderung eines Nutzungsrechtes durch den Kunden entsprechend entwertet werden. Bei diesem Lösungsansatz kann dafür gesorgt werden, dass die erste Signatur in der Signatureinrichtung erst dann gebildet wird, wenn die Entwertung einer entsprechenden Anzahl an Werteinheiten der Signatureinrichtung bestätigt worden ist. Mit anderen Worten muss der Kunde zuerst für die Nutzung der Datenverarbeitungseinheit bezahlen, bevor diese freigegeben wird.

Das oben genannte technische Problem wird ebenfalls durch ein Kommunikationssystem nach Anspruch 8 gelöst.

Das Kommunikationssystem umfasst einen, einem Kunden zugeordneten Computer, in dem eine Datenverarbeitungseinheit implementiert ist. Wie bereits weiter oben erläutert, kann es sich bei der Datenverarbeitungseinheit um Software- und/oder Hardwarekomponenten handeln. Ferner weist der Computer eine Speichereinrichtung auf, in der vorbestimmte Projektdaten wenigstens eines zu verarbeitenden Projekts abgelegt sind. Es

sei angemerkt, dass die vorbestimmten Projektdaten vom Softwareanbieter oder vom Kunden selbst vorher festgelegt werden können. Neben den vorbestimmten, d.h. festen Projektdaten, gibt es variable Projektdaten, die vom Kunden innerhalb eines ausgewählten Projekts geändert werden können, ohne dass eine erneute Freigabe der Datenverarbeitungseinheit angefordert werden müsste. Das Kommunikationssystem umfasst ferner eine dem Computer zugeordnete Nutzungserlaubnis-Erzeugungseinrichtung, die eine erste Signatureinrichtung zum Erzeugen einer ersten Signatur aus den vorbestimmten Projektdaten eines ausgewählten Projekts aufweist. Der Computer weist weiterhin eine Einrichtung zum Verifizieren der ersten Signatur und zur Freigabe der Datenverarbeitungseinheit auf, die die Datenverarbeitungseinheit zum Verarbeiten der zu dem ausgewählten Projekt gehörenden Projektdaten nur dann freigibt, wenn die erste Signatur korrekt ist. Die Verifizierungseinrichtung kann auf einer asymmetrischen Signaturfunktion beruhen, das auch unter dem Namen Public-Key-Kryptografie bekannt ist. Bei der asymmetrischen Signaturfunktion wird jedem Teilnehmer, im vorliegenden Fall dem Kunden und dem Softwareanbieter, ein privater, geheimer Schlüssel und ein sogenannter öffentlicher Schlüssel zugeordnet. Da die asymmetrische Signaturfunktion allgemein bekannt ist, wird hierauf nicht weiter eingegangen.

Gemäß einer vorteilhaften Weiterbildung ist der Computer und die Nutzungserlaubnis-Erzeugungseinrichtung über ein Kommunikationsnetz, beispielsweise das Internet, ein Fernsprechnetz oder ähnliche Netze, die zur Übertragung von Daten geeignet sind, miteinander verbindbar. Demzufolge weisen der Computer und die Nutzungserlaubnis-Erzeugungseinrichtung jeweils eine Schnittstelle zum Anschalten an dieses Kommunikationsnetz auf. Um über das ungesicherte Kommunikationsnetz die vorbestimmten

Projektdaten eines ausgewählten Projektes gesichert übertragen zu können, verfügt der Computer über eine Einrichtung zum kryptografischen Sichern der vorbestimmten Projektdaten, und zwar beispielsweise unter Anwendung einer Hashfunktion. Auf diese Weise bleiben die Projektdaten auch vor der Nutzungserlaubnis-Erzeugungseinrichtung geheim. Hashfunktionen sind allgemein bekannt, so dass eine Erläuterung über Hashfunktionen entfallen kann. Grundprinzip einer Hashfunktion ist es, kryptografisch zu sichernde Daten auf einen sogenannten Hashwert zu komprimieren.

Die Nutzungserlaubnis-Erzeugungseinrichtung ist in der Lage, die vom Computer über das Kommunikationsnetz übertragenen vorbestimmten Projektdaten bzw. deren Hashwert zu signieren und die resultierende erste Signatur über das Kommunikationsnetz zum Computer zu übertragen.

Um den Kunden, der die Nutzung oder Freigabe der Datenverarbeitungseinheit anfordert, identifizieren zu können, weist der Computer eine zweite Signatureinrichtung zum Erzeugen einer zweiten Signatur aus den vorbestimmten Projektdaten auf. Der Computer kann die zweite Signatur und die dazu gehörenden vorbestimmten Projektdaten über ein Kommunikationsnetz zur Nutzungserlaubnis-Erzeugungseinrichtung übertragen. Die Nutzungserlaubnis-Erzeugungseinrichtung ist zum Verifizieren der zweiten Signatur ausgebildet, wobei die erste Signatureinrichtung die erste Signatur nur dann erzeugt, wenn die zweite Signatur korrekt ist.

Alternativ kann die zweite Signatureinrichtung des Computers auch eine zweite Signatur aus den vorbestimmten, kryptografisch gesicherten Projektdaten erzeugen, wobei der Computer dann die zweite Signatur und die dazu gehörenden vorbestimmten, kryptografisch gesicherten Projektdaten über

das Kommunikationsnetz zur Nutzungserlaubnis-Erzeugungseinrichtung überträgt. Wiederum ist die Nutzungserlaubnis-Erzeugungseinrichtung zum Verifizieren der zweiten Signatur ausgebildet, wobei die erste Signatureinrichtung die erste Signatur nur dann erzeugt, wenn die zweite Signatur korrekt ist.

Wenn die Nutzung der Datenverarbeitungseinheit kostenpflichtig ist, kann das Kommunikationssystem eine Einrichtung zum Erzeugen eines Rechnungsdatensatzes in Abhängigkeit der vorbestimmten Projektdaten eines ausgewählten Projektes aufweisen. Die Einrichtung zum Erzeugen eines Rechnungsdatensatzes ist vorzugsweise der ersten Signatureinrichtung zugeordnet. Die erste Signatureinrichtung und die Einrichtung zum Erzeugen eines Rechnungsdatensatzes können in einem dem Softwareanbieter zugeordneten Computer implementiert sein. Wichtig ist, darauf hinzuweisen, dass der Kunde für die Nutzung der Datenverarbeitungseinheit zur Verarbeitung von Projektdaten nur einmal für ein Projekt bezahlen muss, sofern die vorbestimmten Projektdaten nicht verändert werden. Im Rahmen der Verarbeitung eines Projektes können daher alle übrigen, nicht vorbestimmten Projektdaten vom Kunden beliebig häufig verändert werden, ohne dass zusätzliche Kosten anfallen. Erst wenn die vorbestimmten Projektdaten für das zu verarbeitende Projekt geändert werden müssen, fallen Kosten für den Kunden an.

Alternativ kann die einem Softwareanbieter zugeordnete Nutzungserlaubnis-Erzeugungseinrichtung eine Chipkarte sein, die die erste Signatureinrichtung enthält. Dem Computer ist dann eine Chipkarten-Leseeinrichtung zur Aufnahme der Chipkarte zugeordnet.

Für den Fall, dass die Nutzung der Datenverarbeitungseinheit kostenpflichtig sein soll, kann die Chipkarte derart implementiert sein, dass nur eine bestimmte Anzahl an Signaturen erzeugt wird. Beispielsweise weist die Chipkarte einen Zähler mit einem vorbestimmten Zählstand auf, der jeweils um Eins reduziert wird, wenn vorbestimmte Projektdaten eines ausgewählten Projekts signiert werden sollen. Der Zählstand des Zählers entspricht einem Geldwert, den der Kunde im voraus, beispielsweise durch Kauf der Chipkarte bezahlen muß.

Alternativ kann die erste Signatureinrichtung auch im Computer des Kunden implementiert sein.

Um eine kostenpflichtige Nutzung der Datenverarbeitungseinheit zu ermöglichen, ist es auch denkbar, Werteinheiten in einem Speicher des Computers abzulegen, die bei jeder Anforderung einer Nutzung der Datenverarbeitungseinheit entsprechend entwertet werden. Die Werteinheiten muß der Kunde im voraus kaufen.

Die Werteinheiten, bei denen es sich um Zufallszahlen handeln kann, können vom Kunden in den Computer eingegeben werden. Alternativ können die Werteinheiten über das Kommunikationsnetz beim Anbieter der Datenverarbeitungseinheit angefordert und von diesem beispielsweise per E-Mail zum Computer des Kunden übertragen werden.

Die Werteinheiten können zusammen mit den zu signierenden vorbestimmten Projektdaten oder den vorbestimmten, kryptografisch gesicherten Projektdaten zur Nutzungserlaubnis-Erzeugungseinrichtung übertragen und dort entwertet werden, bevor die erste Signatur aus den

vorbestimmten Projektdaten oder den vorbestimmten, kryptografisch gesicherten Projektdaten erzeugt wird. Die Erfindung wird nachfolgend anhand mehrerer Ausführungsbeispiele in Verbindung mit den beiliegenden Zeichnungen näher erläutert.

Es zeigen:

Fig. 1 ein schematisches Blockschaltbild eines Kommunikationssystem gemäß der Erfindung,

Fig. 2 ein schematisches Blockschaltbild eines alternativen Kommunikationssystems gemäß der Erfindung, und

Fig. 3 eine Chipkarte mit integrierter Signatureinrichtung, die an den in Fig. 1 und Fig. 2 dargestellten Computer angeschlossen werden kann.

Fig. 1 zeigt ein beispielhaftes Kommunikationssystem, welches einen bei einem Kunden aufgestellten Computer 10 enthält. Der Computer 10 weist einen Speicher 20 auf, in dem die vorbestimmten Projektdaten wenigstens eines Projektes abgelegt werden können. Bei den vorbestimmten Projektdaten handelt es sich um feste Projektdaten eines Projektes. Darüber hinaus gibt es noch variable Projektdaten, die in einem Speicher 22 abgelegt sein können. Ferner kann der Computer 10 eine Einrichtung 30 zum kryptografischen Sichern vorbestimmter Projektdaten aufweisen. Die kryptografische Sicherungseinrichtung 30 führt hierzu eine Hashfunktion mit den vorbestimmten Projektdaten aus. Als Ergebnis liefert die kryptografische Sicherungseinrichtung 30 einen Hashwert der vorbestimmten Projektdaten, der in einem Speicher 40 abgelegt werden kann. Ferner ist in dem Computer eine Datenverarbeitungseinheit 90 implementiert, die als Hardware- und/oder Softwarekomponente ausgebildet sein kann. In der Datenverarbeitungseinheit 90 ist wiederum eine kryptografische Sicherungseinrichtung 100 vorgesehen, der die

festen Projektdaten eines ausgewählten Projekts zugeführt werden. Die kryptografische Sicherungseinrichtung 100 ist mit einer Verifizierungseinrichtung 110 verbunden.

Gemäß dem Ausführungsbeispiel nach Fig. 1 ist der Computer 10 über ein Kommunikationsnetz, beispielsweise das Internet mit einer einem Softwareanbieter zugeordneten Nutzungserlaubnis-Erzeugungseinrichtung 50 verbunden, die nachfolgend kurz Rechner genannt wird. Der Rechner 50 kann einen Speicher 60 aufweisen, in dem der vom Computer 10 kommende Hashwert der vorbestimmten Projektdaten abgelegt wird. Der Speicher 60 ist mit einer Signatureinrichtung 70 verbunden, die mittels eines geheimen Schlüssels den Hashwert signiert. Die in der Signatureinrichtung 70 erzeugte Signatur I kann in einem Speicher 80 abgelegt werden. Der Rechner 50 überträgt die im Speicher 80 abgelegte Signatur I über das Kommunikationsnetz zum Computer 10. Im Computer 10 wird die empfangene Signatur I der Verifizierungseinrichtung 110 zugeführt. Die Verifizierungseinrichtung 110 basiert vorteilhafterweise auf einer asymmetrischenSignaturfunktion, beispielsweise dem sogenannten RSA-Verfahren. Die Verifizierungseinrichtung 110 ist dazu ausgebildet, mit Hilfe des in der kryptografischen Sicherungseinrichtung 100 erzeugten Hashwertes und der empfangenen Signatur I festzustellen, ob die Signatur I korrekt ist. Stellt die Verifizierungseinrichtung 110 fest, dass die bei ihr eingereichte Signatur I echt ist, d. h. tatsächlich von der ersten Signatureinrichtung stammt, wird die Datenverarbeitungseinheit 90 zur Verarbeitung der zum ausgewählten Projekt gehörenden Projektdaten freigegeben.

In dem Computer 10 kann ein Speicher 170 zum Ablegen von Werteinheiten vorgesehen sein. Diese Werteinheiten werden vom Kunden vorausbezahlt und auf Anforderung des Kunden beispielsweise in dem Rechner 50 erzeugt, über das

Kommunikationsnetz übertragen und in den Speicher 170 geladen. Die Entwertung der Werteinheiten kann in dem Computer 10 erfolgen oder aber dadurch bewirkt werden, dass Werteinheiten aus dem Speicher 170 über das Kommunikationsnetz zu einer Entwerteeinrichtung 180 des Rechners 50 übertragen werden. Die Werteinheiten können verschlüsselt oder unverschlüsselt vom Computer 10 zum Rechner 50 übertragen werden.

Eine vorteilhafte Weiterbildung sieht vor, dass die Signatureinrichtung 70 den vom Computer 10 übertragenen Hashwert erst dann signiert, wenn eine entsprechende Anzahl an Werteinheiten in der Entwertungseinrichtung 180 entwertet worden ist. Die Entwerteeinrichtung 180 liefert hierzu ein entsprechendes Triggersignal an die Signatureinrichtung 70. Auf diese Weise wird sichergestellt, dass die Nutzung der Datenverarbeitungseinheit 90 erst dann freigegeben wird, wenn der Kunde den fälligen Betrag bezahlt hat.

In Fig. 2 ist ein alternatives Kommunikationssystem dargestellt.

Im Unterschied zu dem in Fig. 1 dargestellten Computer 10 weist der in Fig. 2 dargestellte Computer 10 noch eine Signatureinrichtung 130 auf, die den im Speicher 40 abgelegten Hashwert signiert. Diese Signatur II kann in einem Speicher 140 abgelegt werden. Die Signatureinrichtung 130 dient dazu, Softwareanbietern eine Möglichkeit zu geben, zu überprüfen, ob der die Nutzung der Datenverarbeitungseinheit 90 anfordernde Kunde auch tatsächlich der Kunde ist, von dem der Hashwert der vorbestimmten Projektdaten kommt. Zur Prüfung der Signatur II ist in dem Rechner 50 eine Verifizierungseinrichtung 160 implementiert. Vorzugsweise ist der Verifizierungseinrichtung 160 ein Speicher 150 zugeordnet, in dem die von der Signatureinrichtung 130

erzeugte Signatur II abgelegt werden kann. Wie der Rechner 50 nach Fig. 1 weist der in Fig. 2 dargestellte Rechner 50 eine Signatureinrichtung 70, einen Speicher 60 zum Speichern eines vom Computer 10 kommenden Hashwertes sowie einen Speicher 80 zur Speicherung der in der Signatureinrichtung 70 erzeugten Signatur I auf.

Die Verifizierungseinrichtung 160 ist mit der Signatureinrichtung 70 verbunden. Die Signatureinrichtung 70 bildet über den vom Computer 10 kommenden Hashwert eine Signatur I erst dann, wenn die Verifizierungseinrichtung 160 signalisiert, dass die vom Computer 10 kommende Signatur II korrekt ist. Darüber hinaus kann der in Fig. 2 gezeigte Rechner 50 weiterhin eine Einrichtung 120 zum Erstellen eines Rechnungsdatensatzes enthalten. Ein Rechnungsdatensatz wird erzeugt, wenn die Signatureinrichtung 70 eine Signatur I erzeugt hat. Der Rechnungsdatensatz kann vom Rechner 50 über das Kommunikationsnetz zum Computer 10 übertragen und dort beispielsweise als Rechnung auf einem nicht dargestellten Drucker ausgegeben werden.

Fig. 3 zeigt eine alternative Ausführungsform der in Fig. 1 und Fig. 2 gezeigten Signatureinrichtung 70. Danach ist eine Signatureinrichtung 197 in einer Chipkarte 190 implementiert. Die Chipkarte 190 kann in eine nicht dargestellte Chipkarte-Leseeinrichtung eingesetzt werden, die extern an einen Computer 10 angeschlossen werden kann. Die Chipkarten-Leseeinrichtung kann aber auch im Computer 10 selbst implementiert sein. Der Computer 10 weist einen Speicher 20 auf, in dem vorbestimmte Projektdaten wenigstens eines Projekts gespeichert werden können. In einem weiteren Speicher 22 sind die übrigen, variablen Projektdaten wenigstens eines Projekts gespeichert. Ferner weist der Computer 10 eine Datenverarbeitungseinheit 110 mit einer Verifizierungseinrichtung auf.

Die in dem Speicher 20 des Computers 10 gespeicherten festen Projektdaten werden zur Signatureinrichtung 197 der Chipkarte 190 übertragen, sobald der Kunde die Nutzung einer Datenverarbeitungseinheit 90 anfordert. Die festen Projektdaten werden signiert und als Signatur zur Verifizierungseinrichtung 110 übertragen. Wie Fig. 3 weiter zeigt, ist der Speicher 20 ebenfalls mit der Verifizierungseinrichtung 110 verbunden. Es sei angemerkt, dass die Verifizierungseinrichtung 110 als Software und/oder Hardwarekomponente ausgebildet sein kann. Stellt die Verifikationseinrichtung 110 fest, dass die von der Signatureinrichtung 197 kommende Signatur korrekt ist, wird die Datenverarbeitungseinheit 90 zur Verarbeitung der zu einem ausgewählten Projekt gehörenden Projektdaten freigegeben.

Soll die Nutzung der Datenverarbeitungseinheit 90 kostenpflichtig sein, so kann in der Chipkarte 190 ein Zähler 195 implementiert sein, dessen Zählstand einem bestimmten Geldwert entspricht. Der Zählstand wird jeweils um Eins reduziert, wenn die Signatureinrichtung 197 vorbestimmte Projektdaten eines ausgewählten Projekts signiert. Der Kunde kann die Chipkarte 190 mit einem vorbestimmten Zählstand kaufen, so dass er für die projektbezogene, kostenpflichtige Nutzung der Datenverarbeitungseinheit 90 im voraus bezahlt hat.

Die Funktionsweise des Kommunikationssystems wird nachfolgend anhand eines Ausführungsbeispiels in Verbindung mit Fig. 2 näher erläutert.

Angenommen sei, dass der Kunde Lichtwellenleiter zwischen München und Darmstadt verlegen möchte. Zu diesem Projekt gehören mehrere Projektdaten, wie z.B. die Streckenlänge L zwischen München und Darmstadt, Fasertypen

und die Faserdämpfung der zu verwendenden Lichtwellenleiter. Ferner sei angenommen, dass die Projektdaten „Streckenlänge" vom Kunden als feste Projektdaten vorgegeben werden. Die Projektdaten „Fasertyp" und „Faserdämpfung" sind freie, d.h. variable Projektdaten. Die Streckenlänge L zwischen München und Darmstadt wird als feste Projektdaten in den Speicher 20 abgelegt. Die übrigen Projektdaten können im Speicher 22 abgelegt sein, oder bei Bedarf über die Tastatur des Computers 10 eingegeben werden.

Der Kunde möchte nunmehr das Projekt „Verlegung von Lichtwellenleitern zwischen München und Darmstadt" von der Datenverarbeitungseinheit 90 berechnen lassen. Um die Datenverarbeitungseinheit 90 für das ausgewählte Projekt nutzen zu können, muss der Kunde zunächst ein Nutzungsrecht anfordern oder die Freigabe der Datenverarbeitungseinheit beantragen. Die Anforderung der Nutzungsrechte erfolgt zunächst dadurch, dass für die im Speicher 20 abgelegte Streckenlänge L in der kryptografischen Sicherungseinrichtung 30 ein entsprechender Hashwert erzeugt wird. Um den Sicherheitsstand zu erhöhen, wird der Hashwert in der Signatureinrichtung 130 signiert. Anschließend werden sowohl der Hashwert als auch die Signatur II des Hashwertes per E-Mail über das Kommunikationsnetz zum Rechner 50 übertragen. Die Signatureinrichtung 130 kann auf einem Standard-Verfahren, wie z.B. Pretty Good Privacy (PGP) beruhen. Alternativ kann auch bei der Erzeugung des Hashwertes in der kryptografischen Sicherungseinrichtung 40 eine Signaturfunktion durchgeführt werden. Wichtig ist, dass die in der Signatureinrichtung 130 erzeugte Signatur II mit einem geheimen Schlüssel erzeugt wird, der dem Anbieter der Datenverarbeitungseinheit 90 nicht bekannt ist. Der per E-Mail übertragene Hashwert und die Signatur II werden in dem Speicher 60 bzw. 150 des Rechners 50 abgelegt. Anschließend wird die Signatur II der Verifizierungseinrichtung 160

zugeführt, die unter Anwendung bekannter Methoden prüft, ob die in der Signatureinrichtung 130 erzeugte Signatur II korrekt ist. Ist die Signatur II korrekt, wird die Signatureinrichtung 70 veranlasst, den im Speicher 60 abgelegten Hashwert zu signieren. Der signierte Hashwert kann beispielsweise in dem Speicher 80 abgelegt werden. Die Signatureinrichtung 70 verwendet einen geheimen Schlüssel, der unabhängig ist von dem geheimen Schlüssel der Signatureinrichtung 130 des Computers 10. Die im Speicher 80 hinterlegte Signatur I wird beispielsweise per E-Mail über das Kommunikationsnetz dem Computer 10 und von dort der Verifizierungsfunktion 110 zugeführt. Für die Streckenlänge L, die im Speicher 20 abgelegt ist, wird in der kryptografischen Sicherungseinrichtung 100 ein Hashwert erzeugt, der ebenfalls der Verifizierungsfunktion 110 zugeführt wird. Unter Anwendung bekannter asymmetrischer Signaturfunktionen prüft die Verifizierungseinrichtung 110, ob die vom Rechner 50 kommende Signatur I korrekt ist. Ist die Signatur korrekt, wird die Datenverarbeitungseinheit 90 freigeschaltet und die zu dem Projekt „Verlegung von Lichtwellenleitern zwischen München und Darmstadt" gehörenden Projektdaten, die beispielsweise in den Speichern 20 und 22 abgelegt sind, werden zur Verarbeitung in die Datenverarbeitungseinheit 90 eingegeben.

Mit der Erstellung der Signatur I in der Signatureinrichtung 70 wird die Einrichtung 120 veranlasst, einen entsprechenden Rechnungsdatensatz zu erzeugen, der beispielsweise ebenfalls per E-Mail zum Computer 10 übertragen wird. Der Rechnungsdatensatz kann in eine Rechnung umgesetzt und über einen Drucker (nicht dargestellt) ausgegeben werden. Um einen Rechnungsdatensatz in Abhängigkeit von den im Speicher 20 abgelegten vorbestimmten Projektdaten erstellen zu können, werden bestimmte Parameter, wie zum Beispiel Anzahl und Art der für ein ausgewähltes Projekt vorbestimmten Projektdaten,

oder die vorbestimmten Projektdaten selbst vom Computer 10 zur Einrichtung 120 übertragen. Die Parameter können verschlüsselt zum Rechner 50 übertragen werden. Der Rechner 50 oder die Einrichtung 120 ist in der Lage, die verschlüsselten Parameter wieder zu entschlüssen.

Patentansprüche

1. Verfahren zur Freigabe einer Datenverarbeitungseinheit (90) zur Verarbeitung von Projektdaten eines Projekts, nach welchem
ein Kunde die Nutzungserlaubnis für die Nutzung einer Datenverarbeitungseinheit (90) zur Verarbeitung der zu einem vorbestimmten Projekt gehörenden Projektdaten anfordert,
eine erste Signatur (I) erzeugt wird, indem vorbestimmte, zu dem Projekt gehörende Projektdaten signiert werden,
die erste Signatur (I) auf Korrektheit hin verifiziert wird, und
die Datenverarbeitungseinheit (90) nur dann freigegeben wird, die zum ausgewählten Projekt gehörenden Projektdaten zu verarbeiten, wenn die erste Signatur (I) als korrekt verifiziert worden ist.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
die erste Signatur (I) in einer Einrichtung zur Erzeugung einer Nutzungserlaubnis (50, 70) erzeugt wird, wobei die vorbestimmten Projektdaten über ein Kommunikationsnetz zur Nutzungserlaubnis-Erzeugungseinrichtung (50, 70) übertragen werden.

3. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
die vorbestimmten Projektdaten kryptografisch gesichert werden,
die vorbestimmten, kryptografisch gesicherten Projektdaten über ein Kommunikationsnetz zur Nutzungserlaubnis-Erzeugungseinrichtung (50, 70) übertragen werden und dass
die erste Signatur (I) erzeugt wird, indem die

vorbestimmten kryptografisch gesicherten Projektdaten von der Nutzungserlaubnis-Erzeugungseinrichtung (50, 70) signiert werden.

4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass eine zweite Signatur (II) erzeugt wird, indem die vorbestimmten Projektdaten signiert werden, dass die vorbestimmten Projektdaten und die zweite Signatur (II) zur Nutzungserlaubnis-Erzeugungseinrichtung (50) übertragen werden, dass die zweite Signatur auf Korrektheit hin verifiziert wird, und dass die erste Signatur (I) aus den vorbestimmten Projektdaten nur erzeugt wird, wenn die zweite Signatur (II) korrekt ist.

5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass eine zweite Signatur (II)erzeugt wird, indem die vorbestimmten, kryptografisch gesicherten Projektdaten signiert werden, dass die vorbestimmten, kryptografisch gesicherten Projektdaten und die zweite Signatur (II) zur Nutzungserlaubnis-Erzeugungseinrichtung (50) übertragen werden, dass die zweite Signatur (II) auf Korrektheit hin verifiziert wird, und dass die erste Signatur (I) aus den vorbestimmten, kryptografisch gesicherten Projektdaten nur erzeugt wird, wenn die zweite Signatur korrekt ist.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass für den Kunden in Abhängigkeit von den vorbestimmten

Projektdaten ein Rechnungsdatensatz zur Nutzung der Datenverarbeitungseinheit (90) erzeugt wird.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass einem Kunden mehrere Werteinheiten zur Freigabe der Datenverarbeitungseinheit (90) für mehrere Projekte zugeordnet werden, die bei Anforderung eines Nutzungsrechts durch den Kunden entsprechend entwertet werden.

8. Kommunikationssystem zur Freigabe einer Datenverarbeitungseinheit zur Verarbeitung von Projektdaten eines ausgewählten Projekts, mit einem einem Kunden zugeordneten Computer (10), in dem eine Datenverarbeitungseinheit (90) implementiert ist und der eine Speichereinrichtung (20) aufweist, in der vorbestimmte Projektdaten wenigstens eines zu verarbeitenden Projekts abgelegt sind, einer dem Computer (10) zugeordneten Nutzungserlaubnis-Erzeugungseinrichtung (50), die eine ersten Einrichtung (70) zum Erzeugen einer ersten Signatur (I) aus den vorbestimmten Projektdaten eines ausgewählten Projekts enthält, wobei der Computer (10) eine Einrichtung (110) zum Verifizieren der ersten Signatur (I) und zum Freigeben der Datenverarbeitungseinheit (90) aufweist, die die Datenverarbeitungseinheit (90) zum Verarbeiten der zu dem ausgewählten Projekt gehörenden Projektdaten nur dann freigibt, wenn die erste Signatur (I) korrekt ist.

9. Kommunikationssystem nach Anspruch 8, dadurch gekennzeichnet, dass der Computer (10) eine Schnittstelle zum Anschalten an

ein Kommunikationsnetz und eine Einrichtung (30) zum kryptografischen Sichern der vorbestimmten Projektdaten, insbesondere unter Anwendung einer Hashfunktion, aufweist, und dass
die Nutzungserlaubnis-Erzeugungseinrichtung (50) eine Schnittstelle zum Anschalten an das Kommunikationsnetz aufweist, so dass die erste Signatur (I) über das Kommunikationsnetz zum Computer (10) übertragen werden kann.

10. Kommunikationsnetz nach Anspruch 8,
dadurch gekennzeichnet, dass
dem Computer (10) eine zweite Signatureinrichtung (130) zum Erzeugen einer zweiten Signatur (II) aus den vorbestimmten Projektdaten zugeordnet ist, dass
der Computer (10) zum Übertragen der zweiten Signatur (II) und der dazugehörenden vorbestimmten Projektdaten über ein Kommunikationsnetz zur Nutzungserlaubnis-Erzeugungseinrichtung (50) ausgebildet ist, und dass
die Nutzungserlaubnis-Erzeugungseinrichtung (50) eine Einrichtung (160) zum Verifizieren der zweiten Signatur (II) aufweist, wobei die erste Signatureinrichtung (70) die erste Signatur (I) nur erzeugt, wenn die zweite Signatur (II) korrekt ist.

11. Kommunikationsnetz nach Anspruch 9,
dadurch gekennzeichnet, dass
dem Computer (10) eine zweite Signatureinrichtung (130) zum Erzeugen einer zweiten Signatur (II) aus den vorbestimmten, kryptografisch gesicherten Projektdaten zugeordnet ist, dass
der Computer (10) zum Übertragen der zweiten Signatur (II) und der dazugehörenden vorbestimmten, kryptografisch gesicherten Projektdaten über das Kommunikationsnetz zur Nutzungserlaubnis-Erzeugungseinrichtung (50) ausgebildet

ist, und dass
die Nutzungserlaubnis-Erzeugungseinrichtung (50) eine Einrichtung (160) zum Verifizieren der zweiten Signatur (II) aufweist, wobei die erste Signatureinrichtung (70) die erste Signatur (I) nur erzeugt, wenn die zweite Signatur (II) korrekt ist.

12. Kommunikationssystem nach einem der Ansprüche 8 bis 11, gekennzeichnet durch
eine Einrichtung (120) zum Erzeugen eines Rechnungsdatensatzes für den Kunden zur Nutzung der Datenverarbeitungseinheit (90) in Abhängigkeit der vorbestimmten Projektdaten eines ausgewählten Projekts.

13. Kommunikationssystem nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, dass
die Nutzungserlaubnis-Erzeugungseinrichtung eine Chipkarte (190) ist, in der die erste Signatureinrichtung (197) implementiert ist und die eine vorbestimmte Anzahl an ersten Signaturen erzeugen kann, und dass
dem Computer (10) eine Chipkarten-Leseeinrichtung zugeordnet ist.

14. Kommunikationssystem nach einem der Ansprüche 8 bis 13, gekennzeichnet durch
einen dem Computer (10) zugeordneten Speicher (170), in dem für wenigstens einen Kunden wenigstens eine Werteinheit zur kostenpflichtigen Freigabe der Datenverarbeitungseinheit (90) für die Verarbeitung von Projektdaten wenigstens eines ausgewählten Projekts gespeichert sind, und
eine Einrichtung (180) zum Entwerten der Werteinheiten.

Zusammenfassung

Die Erfindung betrifft ein Verfahren und ein Kommunikationssystem zur Freigabe einer Datenverarbeitungseinheit zur Verarbeitung von Projektdaten eines ausgewählten Projekts.

Um eine projektabhängige Freigabe einer Datenverarbeitungseinheit (90) zu erhalten, fordert ein Kunde ein Nutzungsrecht für die Datenverarbeitungseinheit (90) zur Verarbeitung der zu einem vorbestimmten Projekt gehörenden Projektdaten an. Danach wird eine erste Signatur (I) erzeugt, indem vorbestimmte, zu dem Projekt gehörende Projektdaten von einer Signatureinrichtung (70) signiert werden. Die erste Signatur (I) wird auf Korrektheit hin verifiziert. Die Datenverarbeitungseinheit (90) wird nur dann freigegeben, die zum ausgewählten Projekt gehörenden Projektdaten zu verarbeiten, wenn die erste Signatur (I) als korrekt verifiziert worden ist.

(Fig. 2)

Fig. 1

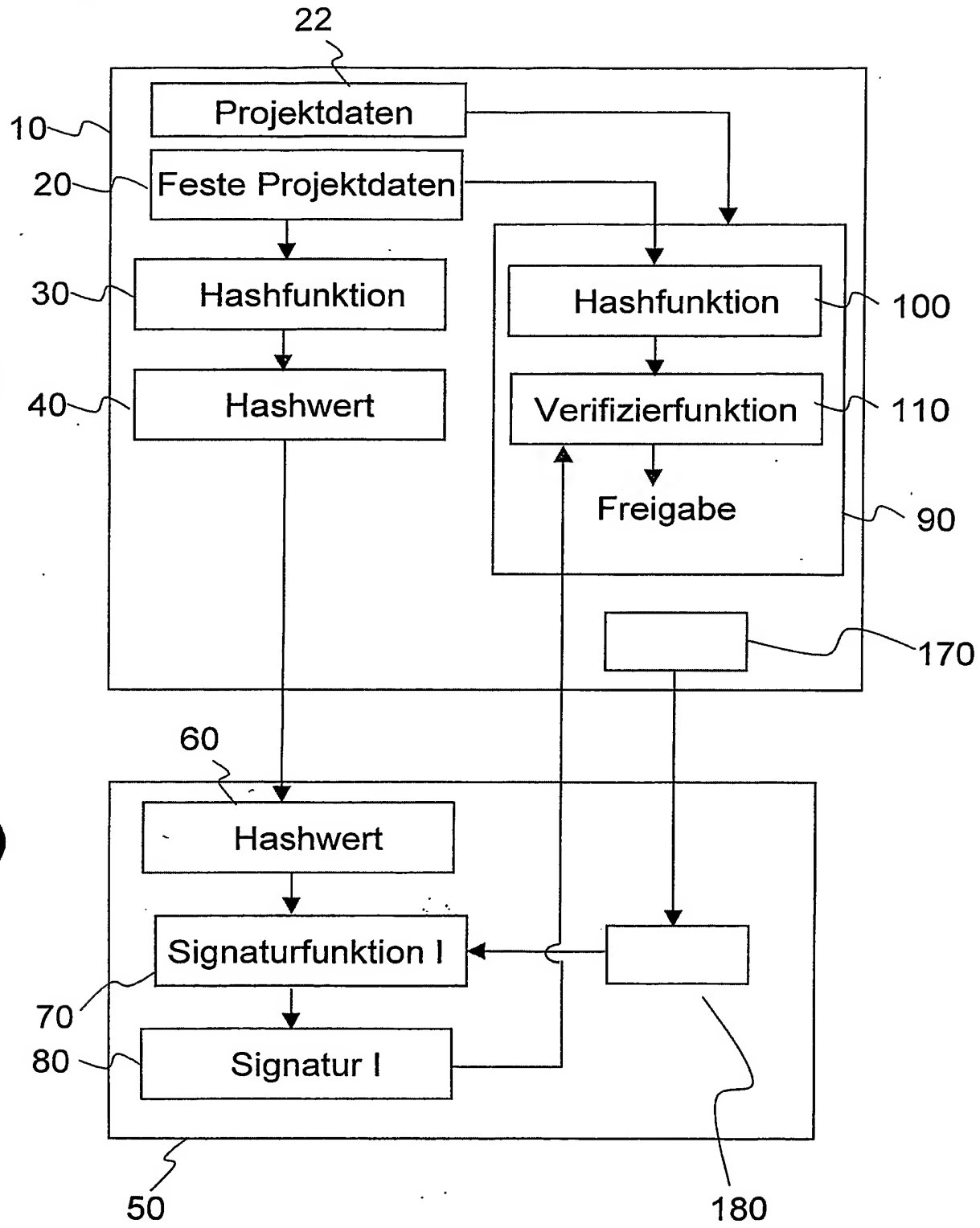

22
Projektdaten
10
20
Feste Projektdaten
30
Hashfunktion
40
Hashwert
Hashfunktion
100
Verifizierfunktion
110
Freigabe
90
170
60
Hashwert
Signaturfunktion I
70
80
Signatur I
50
180

Fig. 2

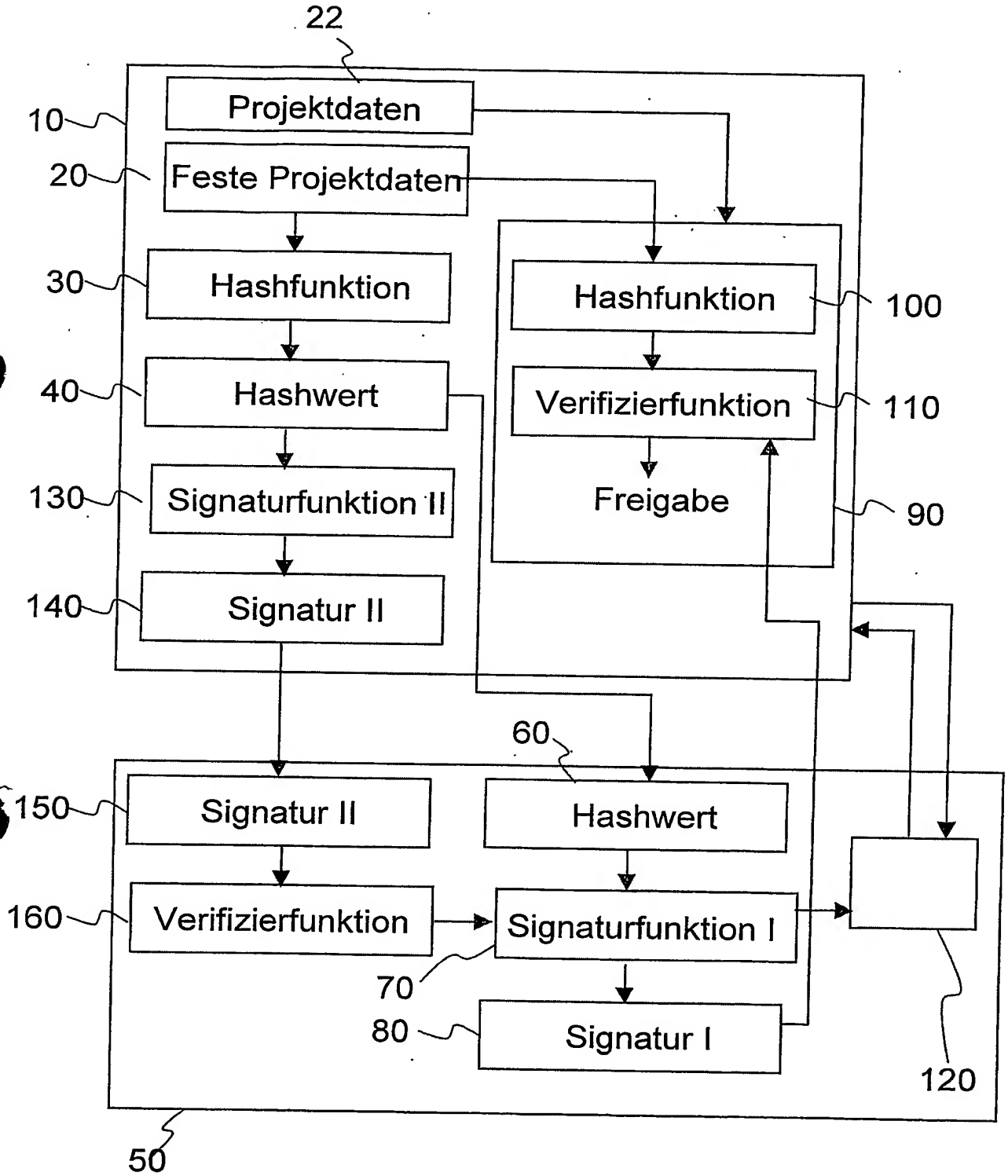
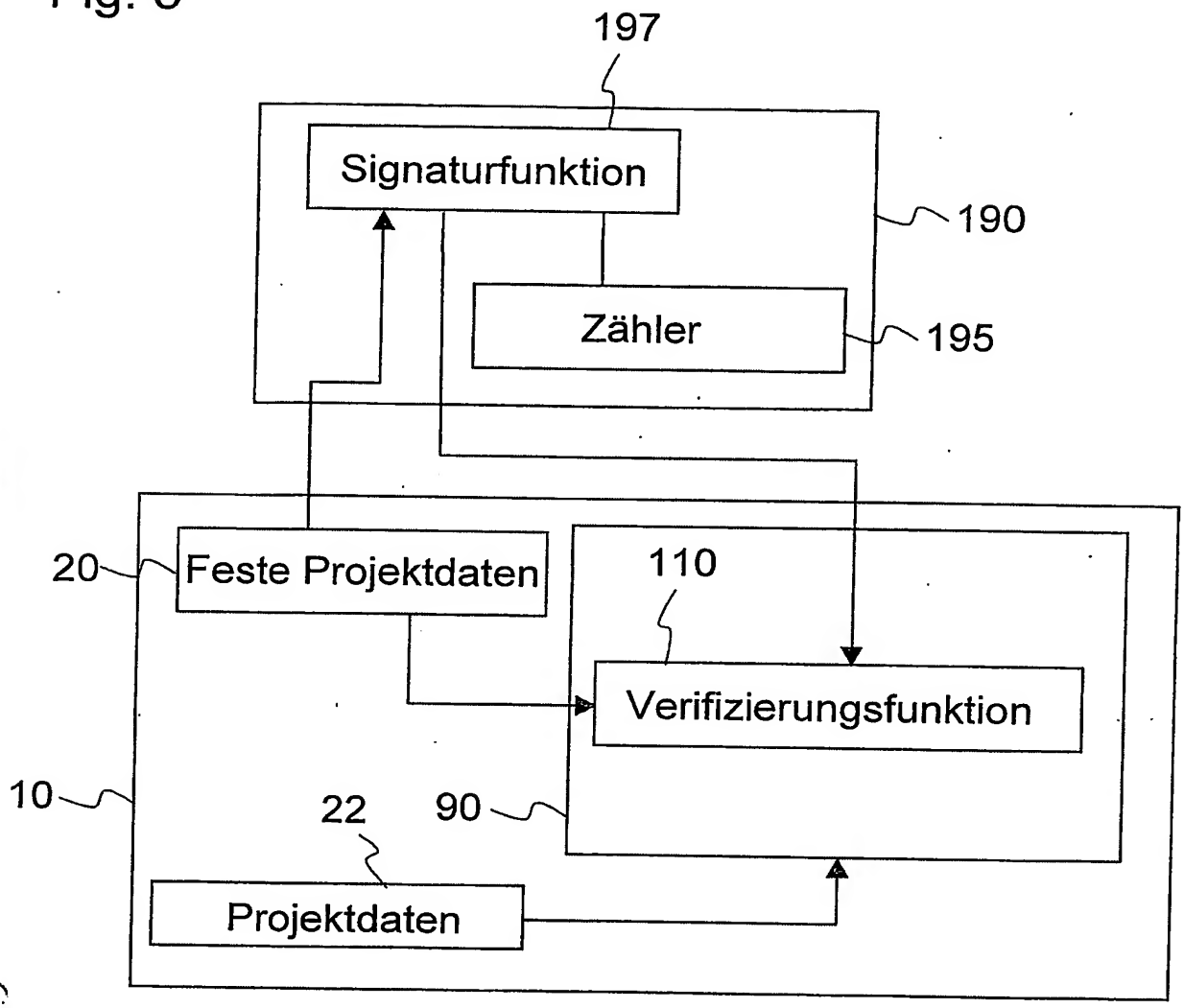

22
Projektdaten
10
20
Feste Projektdaten
30
Hashfunktion
40
Hashwert
130
Signaturfunktion II
140
Signatur II
Hashfunktion
100
Verifizierfunktion
110
Freigabe
90
60
150
Signatur II
Hashwert
160
Verifizierfunktion
Signaturfunktion I
70
80
Signatur I
120
50

Fig. 3


197
Signaturfunktion
190
Zähler
195
20
Feste Projektdaten
110
Verifizierungsfunktion
10
22
90
Projektdaten